SoC Security:
Making a Case for Automation

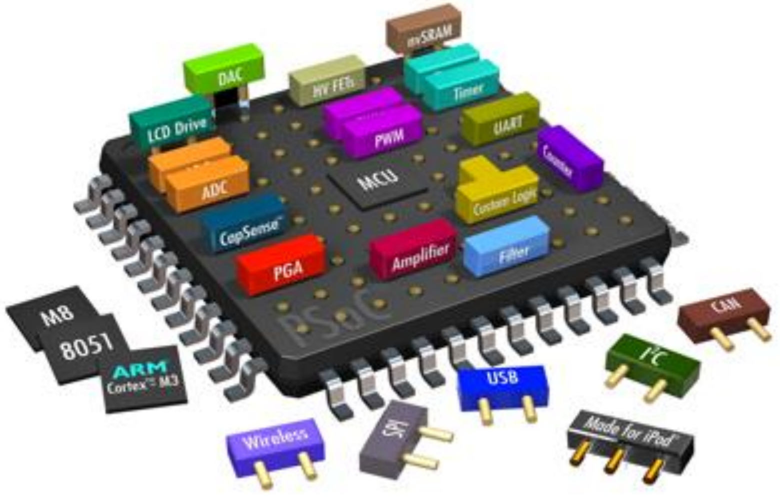
Beau Bakken

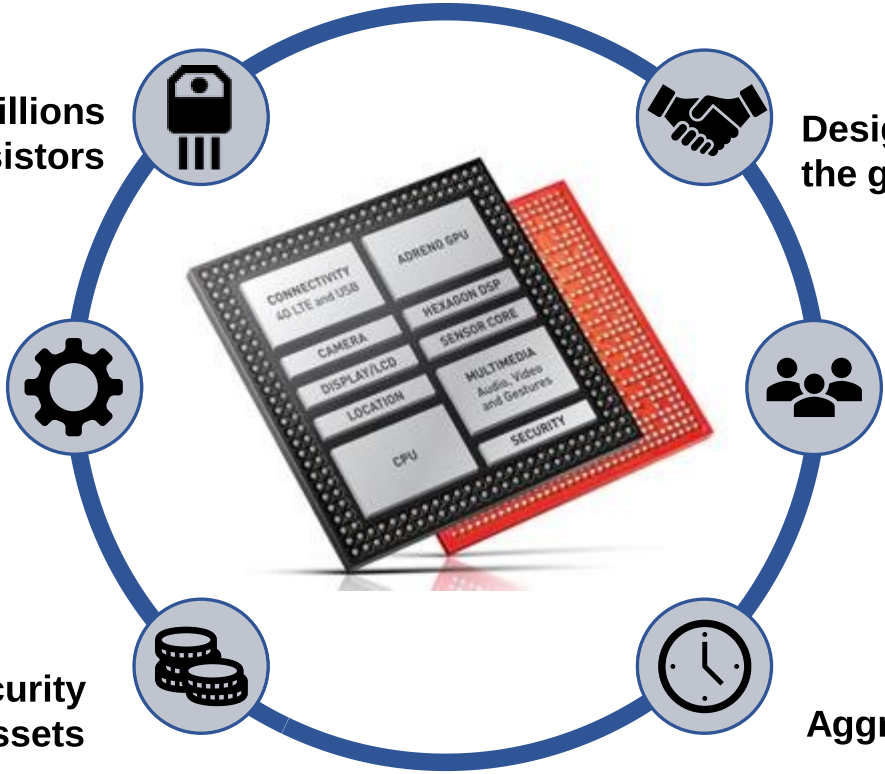
www.caspiatechnologies.com

Caspia Technologies

End-to-End Security Solutions for Electronics Supply Chain

SoC Security





Tens of billions transistors

Designed around the globe

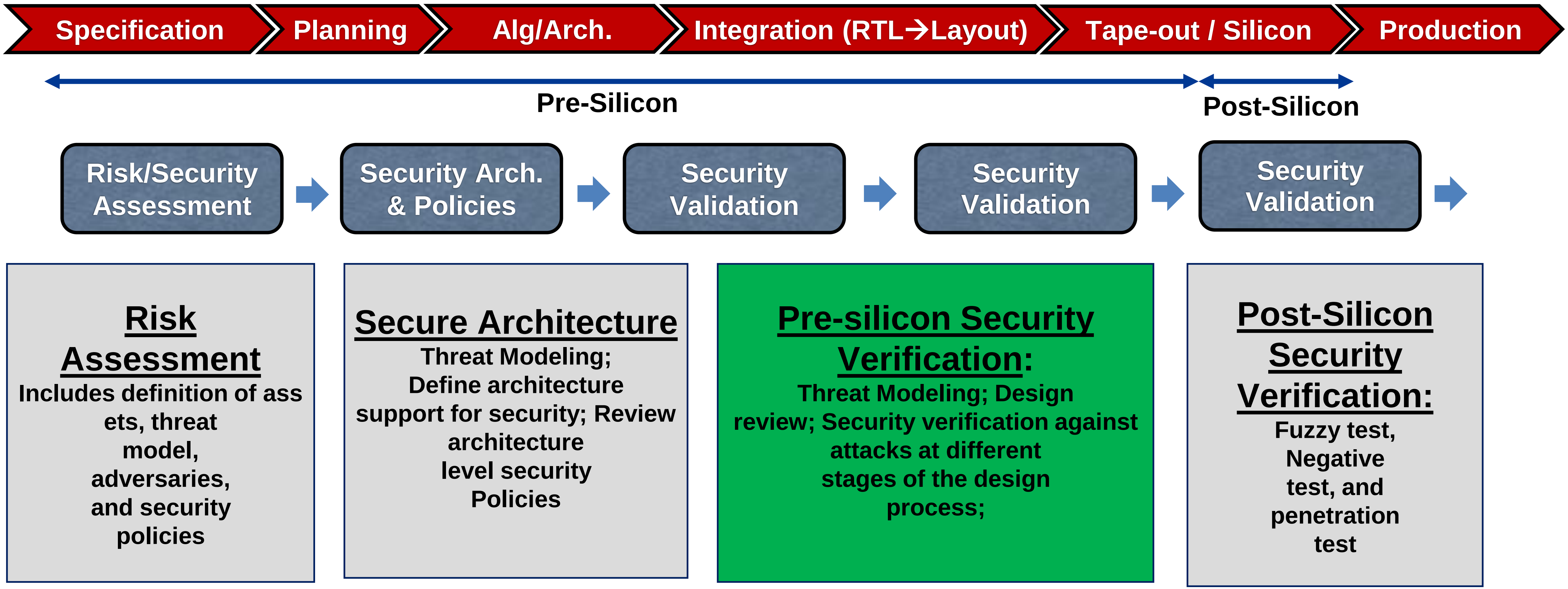
Many custom/legacy functionality

Tens of IPs from 3P vendors

Many security critical assets

Aggressive time-to-market

SDL: Security Development Life-cycle



Specification → Planning → Alg/Arch. → Integration (RTL→Layout) → Tape-out / Silicon → Production

Pre-Silicon

Post-Silicon

Risk/Security Assessment → Security Arch. & Policies → Security Validation → Security Validation → Security Validation →

Risk Assessment
Includes definition of ass ets, threat model, adversaries, and security policies

Secure Architecture
Threat Modeling; Define architecture support for security; Review architecture level security Policies

Pre-silicon Security Verification:
Threat Modeling; Design review; Security verification against attacks at different stages of the design process;

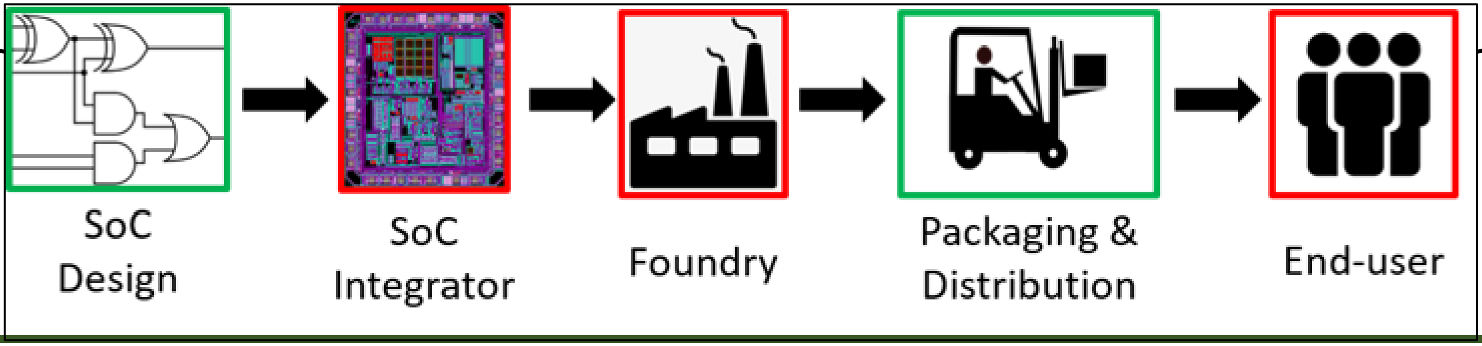
Post-Silicon Security Verification:
Fuzzy test, Negative test, and penetration test

Solutions

Protect the IP

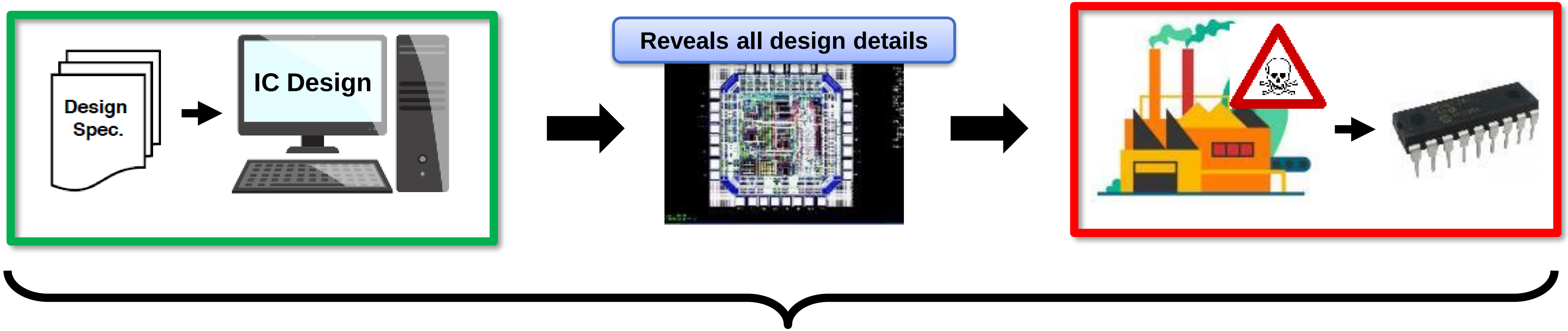
Protect the Assets

Protect the Lifecycle


SoC Design → SoC Integrator → Foundry → Packaging & Distribution → End-user

Protecting Hardware IPs

Insecure Design / Manufacturing Flow



Insider IP Theft

What: Insiders get easy access to the IP

Where: Design flow

Overproduction

What: More chips are produced than agreed upon

Where: Fabrication facilities

Leaked Design File

What: Design ends up in hands of an unauthorized entity

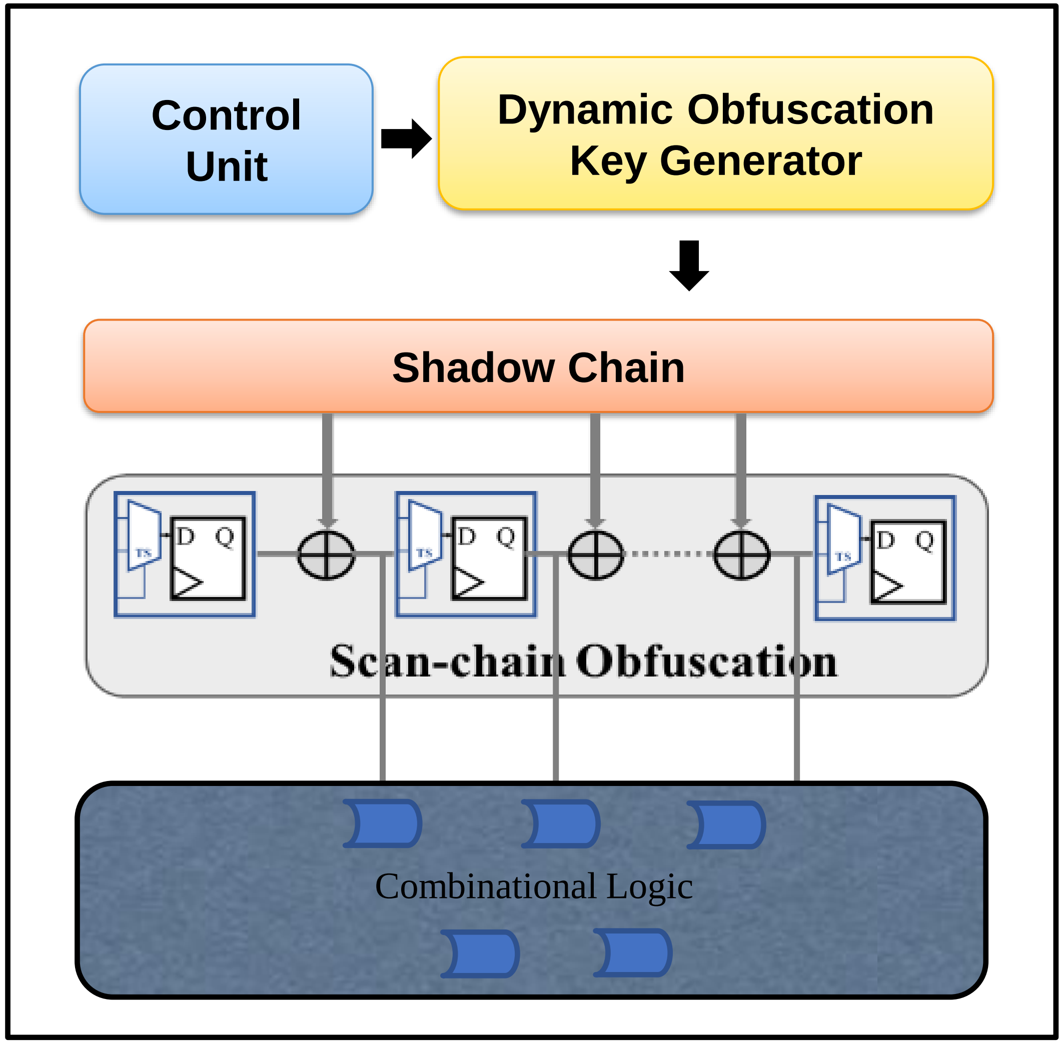
Where: Rogue employee, outside hacker, compromised software, foundry

Reverse Engineering

What: Chip is reversed engineered, and the design IP is extracted

Where: Customer

IPPx: Structural and Functional Locking



- Fetches seed for LFSR
- Controls other modules

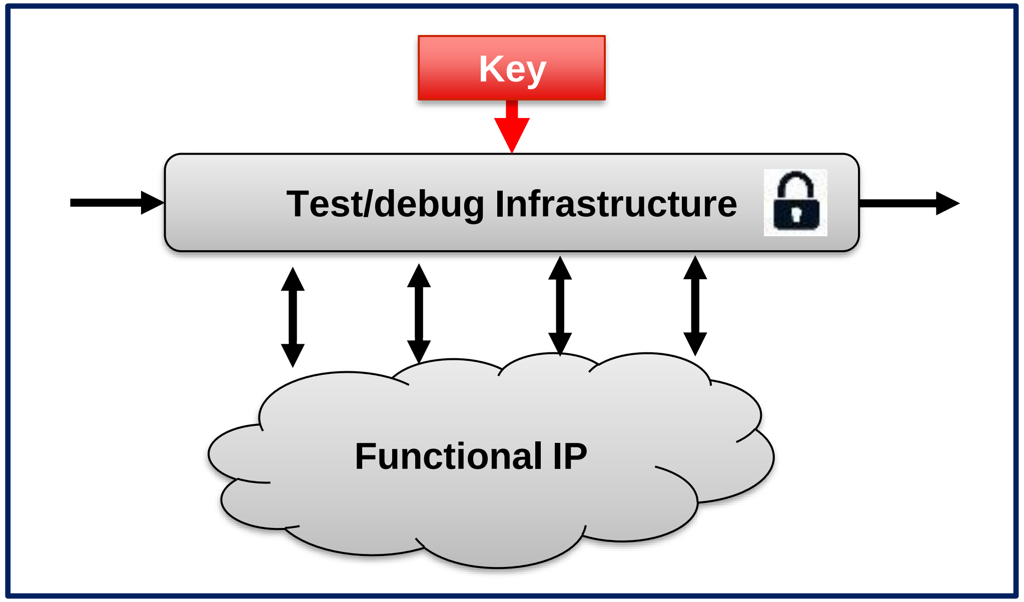
- Dynamically generates obfuscation key (LFSR)

- Prevents unscrambled data from scanned out

- Scrambles scan-in and scan-out patterns

- Locks function by creating black holes forced vis scan chain

IPPx: Test Access Control

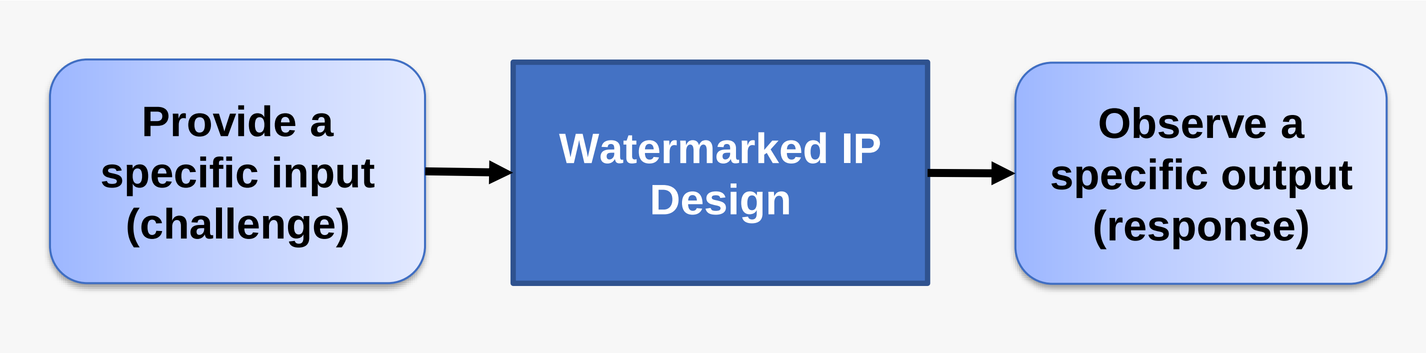


- Scan locking obfuscates the input/output shifted though DFT
- Only authorized users know the key to decrypt the values

Content	Unlocked Design	Locked Design
Pattern Shifted In	**1001**	**1001**
Values delivered to IP	**1001**	**1100**
Values from IP	**0101**	**0001**
Pattern Shifted Out	**0101**	**0110**

Transformation only authorized users will know

IPPx: Watermarking



Provide a specific input (challenge)
Watermarked IP Design
Observe a specific output (response)

Definition: Altering a piece of data to embed identifying information

Goal: Provide proof of ownership

- Uniquely identify IP cores to deter IP piracy
- Trace pirated IPs back to their source

Principals:

- Not easily perceivable
- Hard to remove by adversary
- Easy to identify for the author
- Challenge-Response function is secret

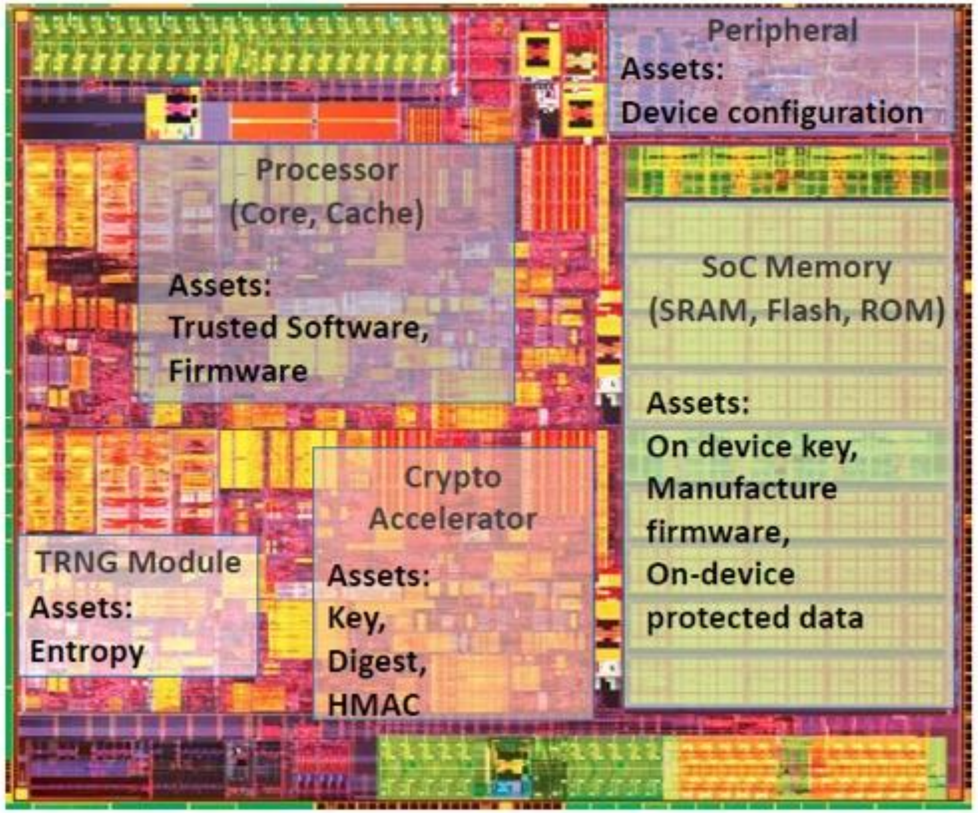
Protecting Assets

Security Assets

Asset: A resource of value worth protecting from an adversary

Security Assets in SoCs:

- On-device keys (developer/OEM)
- Device configuration
- Manufacturer Firmware
- Application software
- On-device sensitive data
- Communication credentials
- Random number or entropy
- E-fuse,
- PUF, and more…



Source: Intel

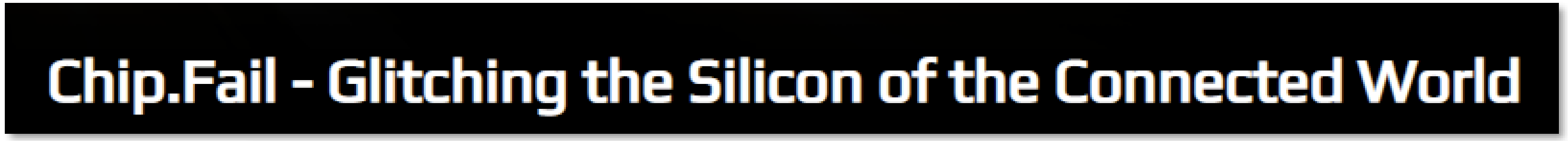
Protect Assets: Strong Algorithms, Weak Implementation

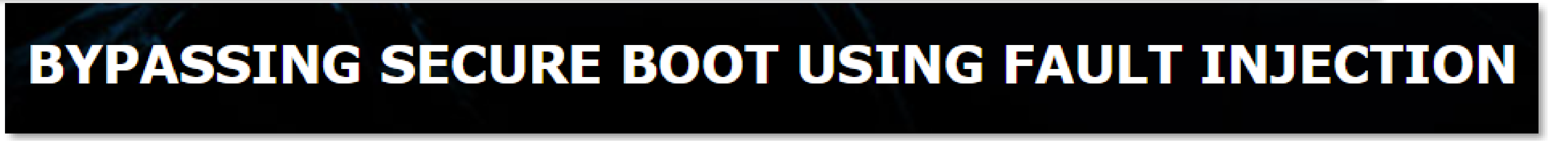
Strong Algorithm & Architecture

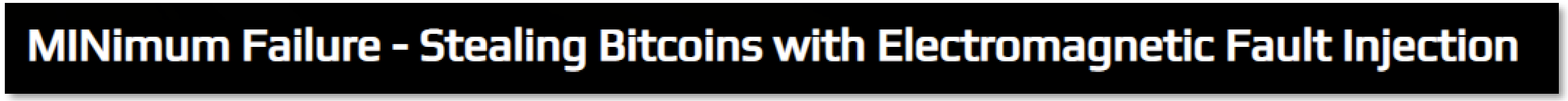
Weak Implementation & Execution

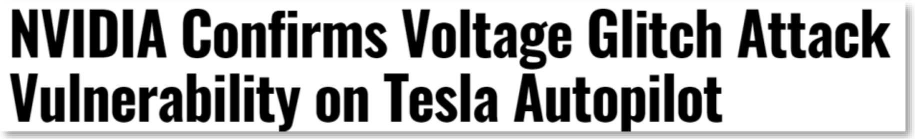
Algorithms, architectures, and policies could be impacted by design methods that do not understand Security!

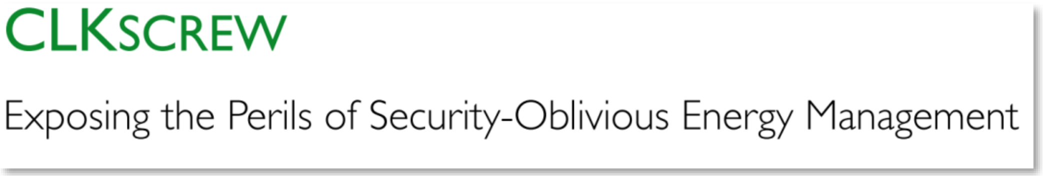
The Rise of Fault Injection


Chip.Fail - Glitching the Silicon of the Connected World


BYPASSING SECURE BOOT USING FAULT INJECTION


MINimum Failure - Stealing Bitcoins with Electromagnetic Fault Injection

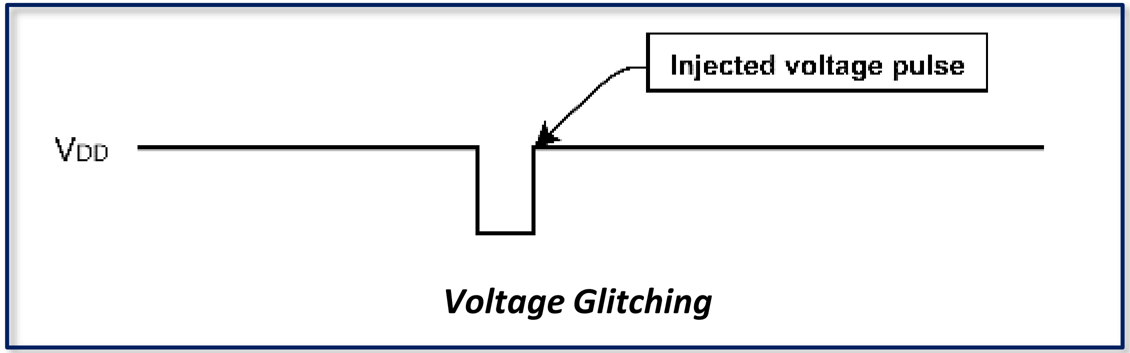

NVIDIA Confirms Voltage Glitch Attack Vulnerability on Tesla Autopilot


CLKSCREW

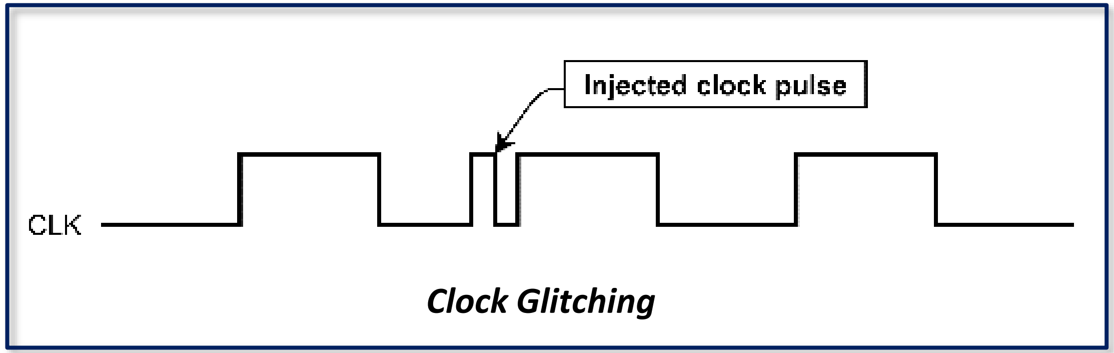
Exposing the Perils of Security-Oblivious Energy Management

...

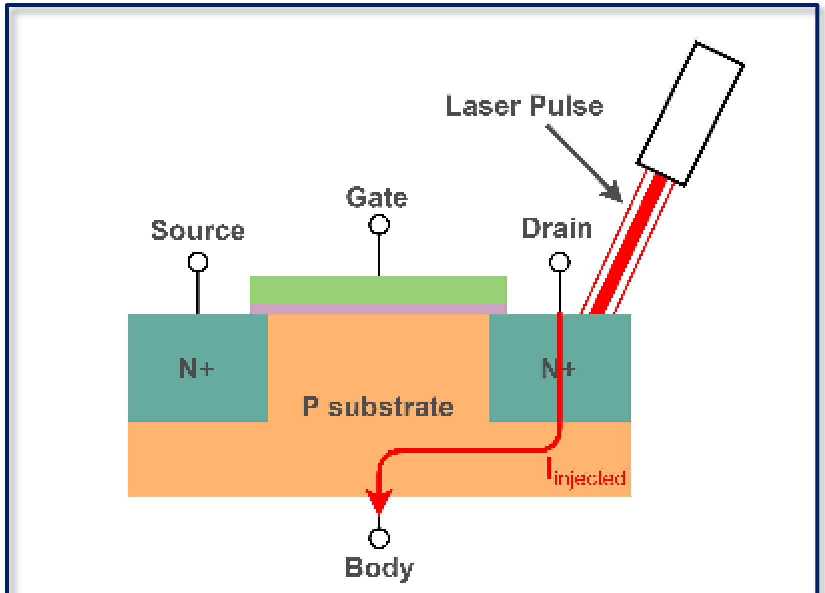
Fault Injection Techniques



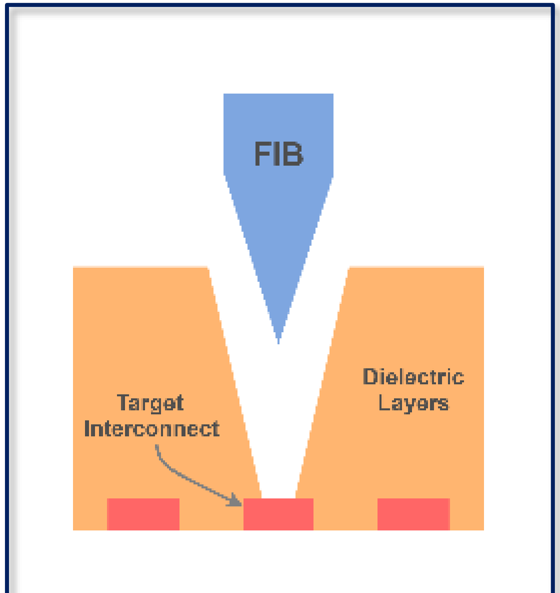
Voltage Glitching



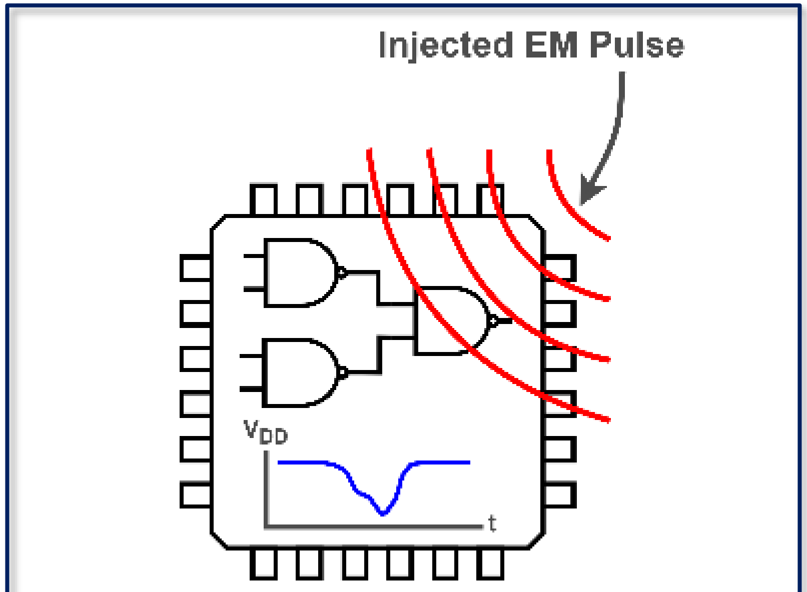
Clock Glitching



Laser Fault Injection (LFI)



Focused Ion Beam (FIB)

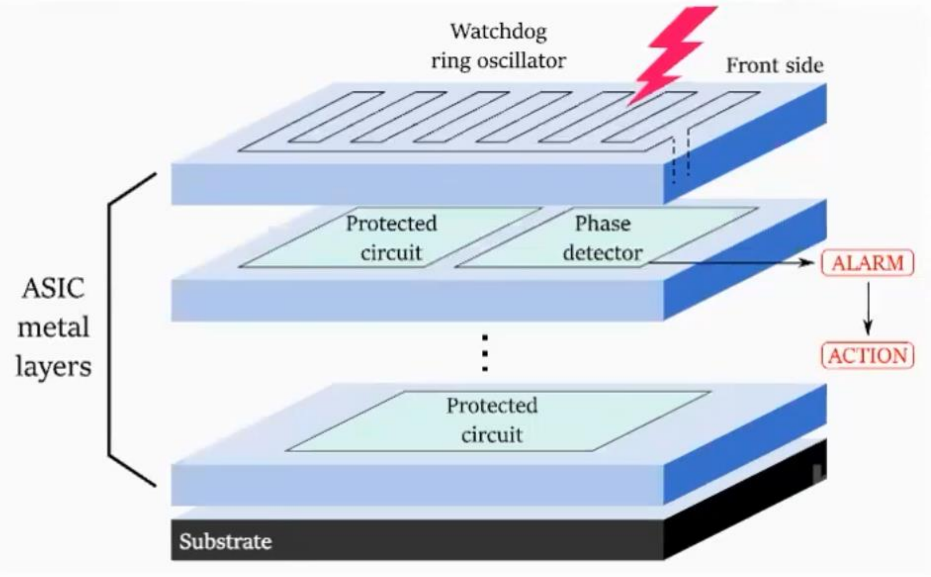


Electromagnetic Fault Injection (EMFI)

Existing Countermeasures

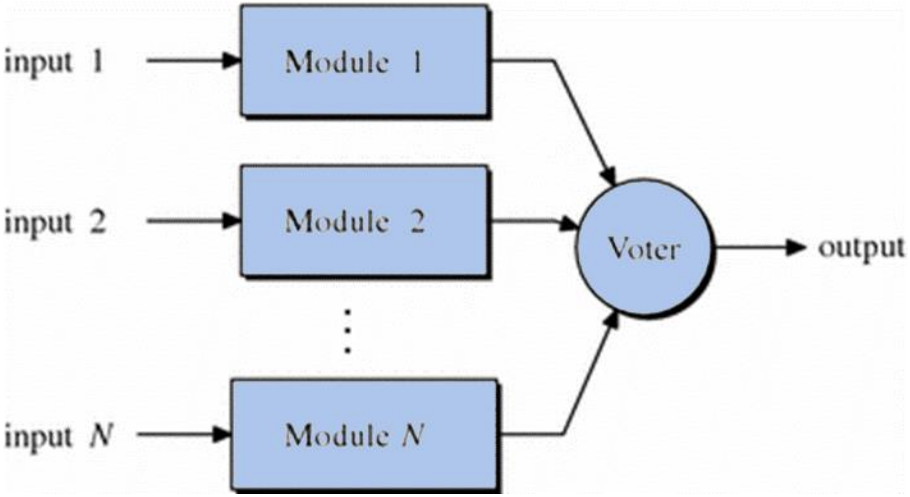
Intrusion Detection

- Example – Sensors
- Disadvantages:
  - Large overhead impact
  - Not localized to specific security feature



Error Detection

- Example – Hardware/time redundancy
- Disadvantages:
  - Large overhead (area/time)
  - Not localized to specific security feature

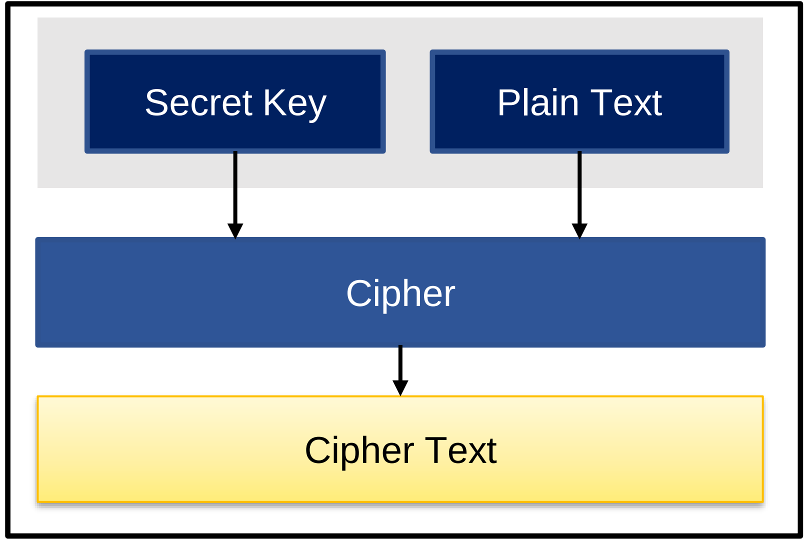


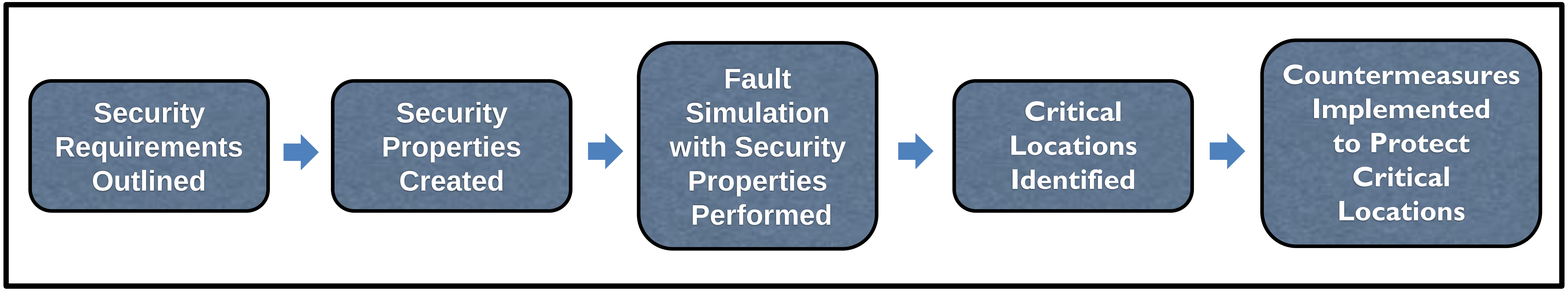
AFIx: Protect Security Properties

Security Properties: Behaviors that must be implemented to maintain security of the design

- **Example SP:** Done signal should not be raised early during AES encryption

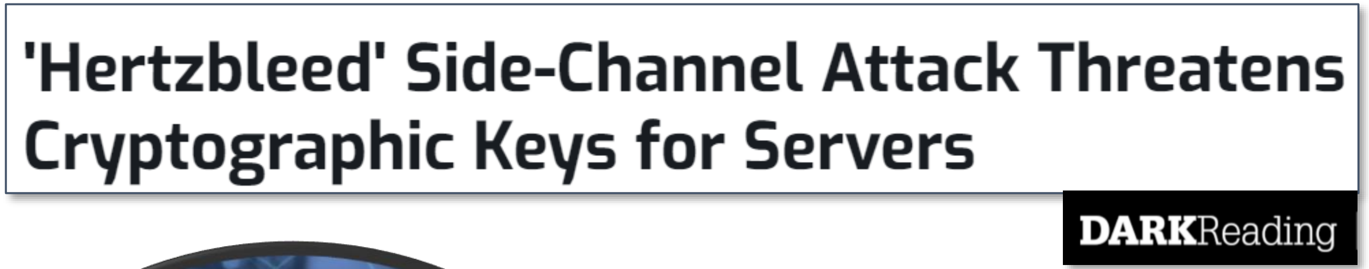
AES Design




Security Requirements Outlined
Security Properties Created
Fault Simulation with Security Properties Performed
Critical Locations Identified
Countermeasures Implemented to Protect Critical Locations

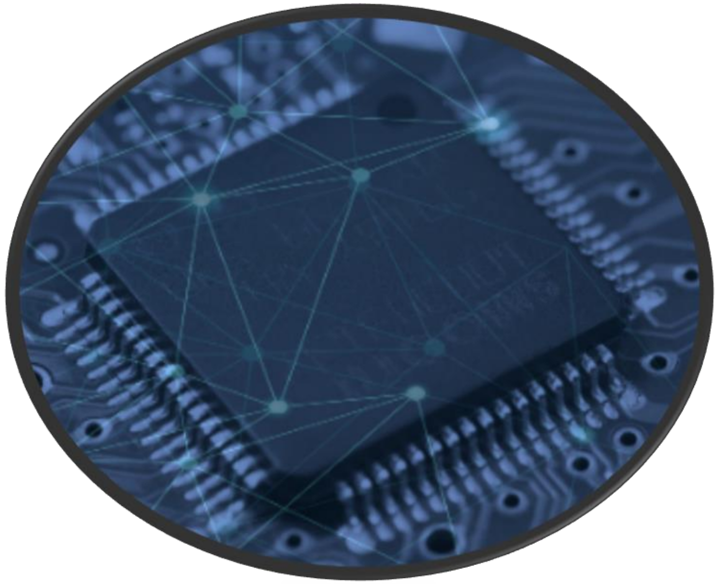
Side-Channel Analysis

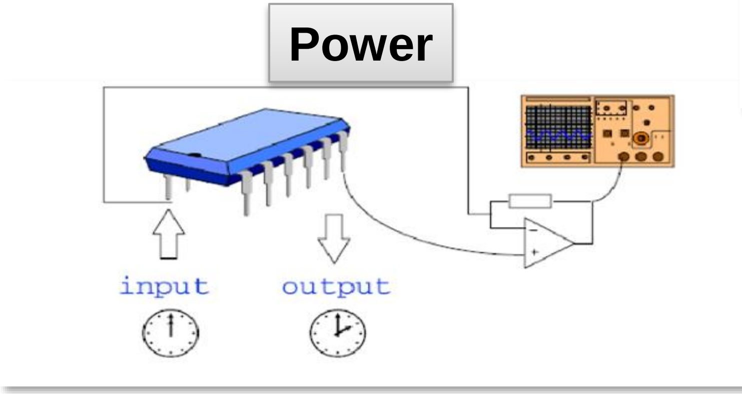
Side-channel analysis is a ***powerful attack***

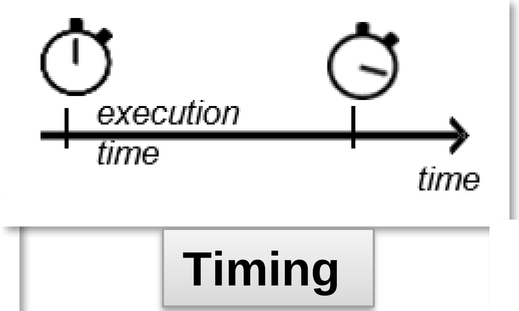


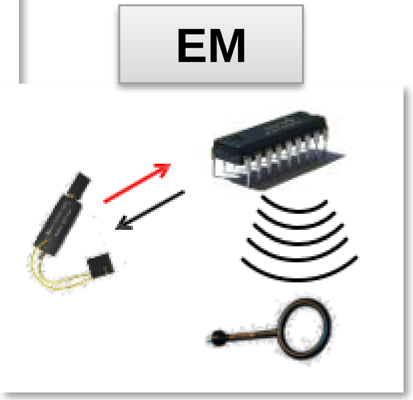
'Hertzbleed' Side-Channel Attack Threatens Cryptographic Keys for Servers

DARKReading





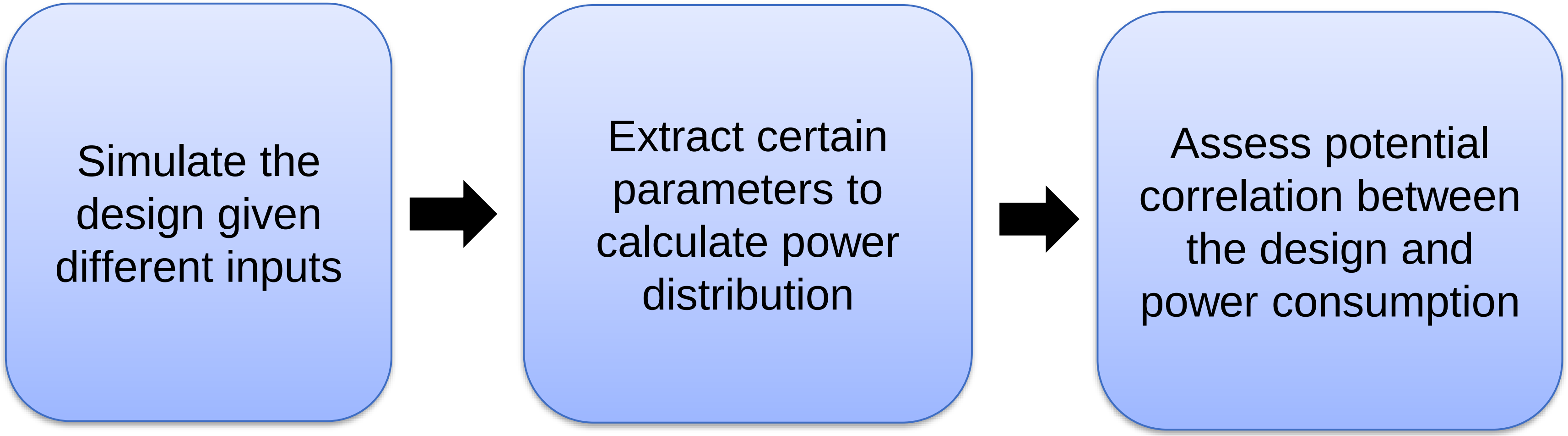




SCMx: Power Side-Channel Assessment

- Early design-stage assessment (RTL) allows greatest flexibility for protection
- Need for metrics to drive design enhancements

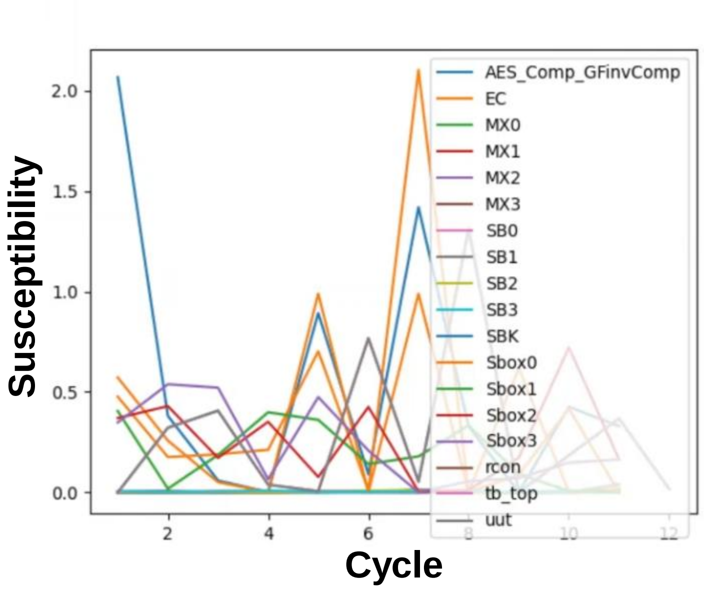
Power Profiling



Simulate the design given different inputs

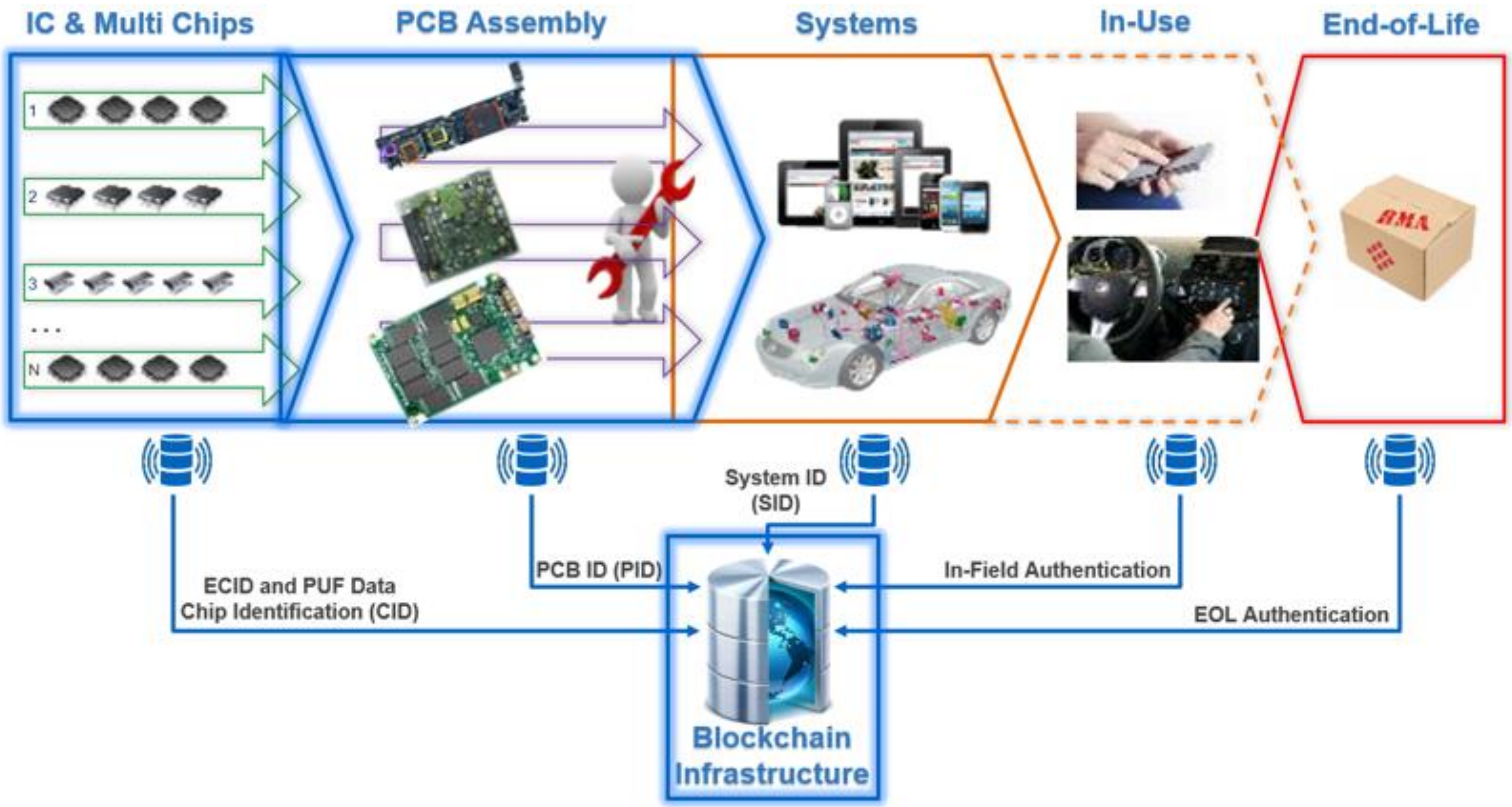
Extract certain parameters to calculate power distribution

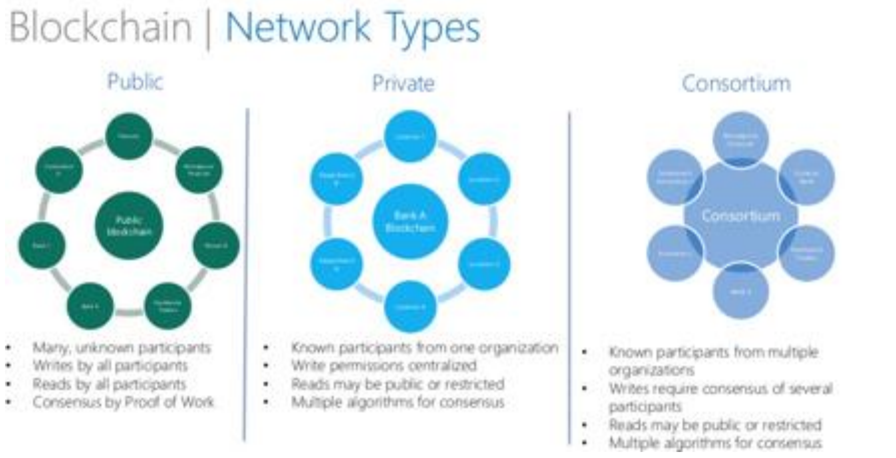
Assess potential correlation between the design and power consumption



Protecting Lifecycle

Device-to-System

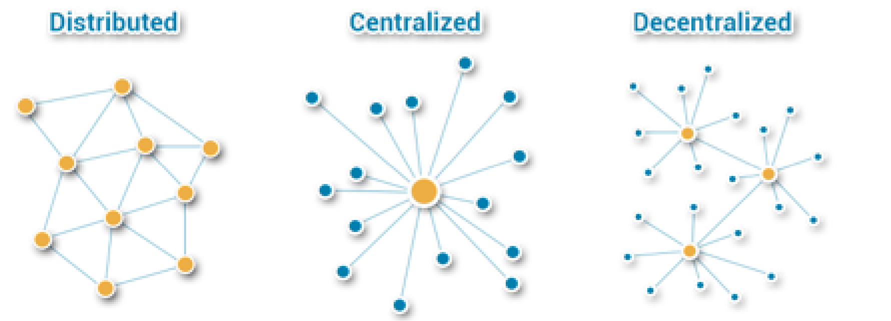




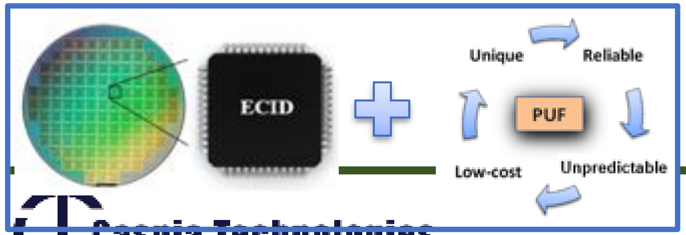
- Many, unknown participants
- Writes by all participants
- Reads by all participants
- Consensus by Proof of Work

- Known participants from one organization
- Write permissions centralized
- Reads may be public or restricted
- Multiple algorithms for consensus

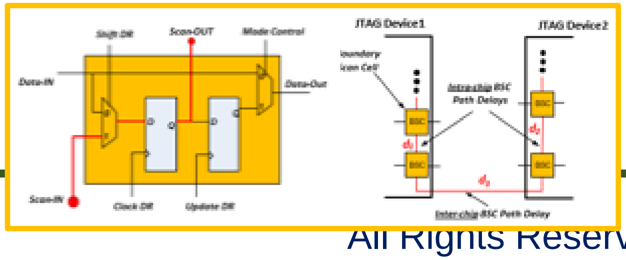
- Known participants from multiple organizations
- Writes require consensus of several participants
- Reads may be public or restricted
- Multiple algorithms for consensus



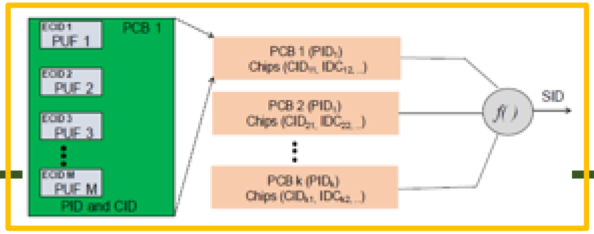
IC Authentication



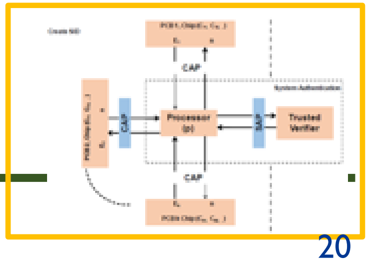
PCB Authentication



Subsystem Authentication

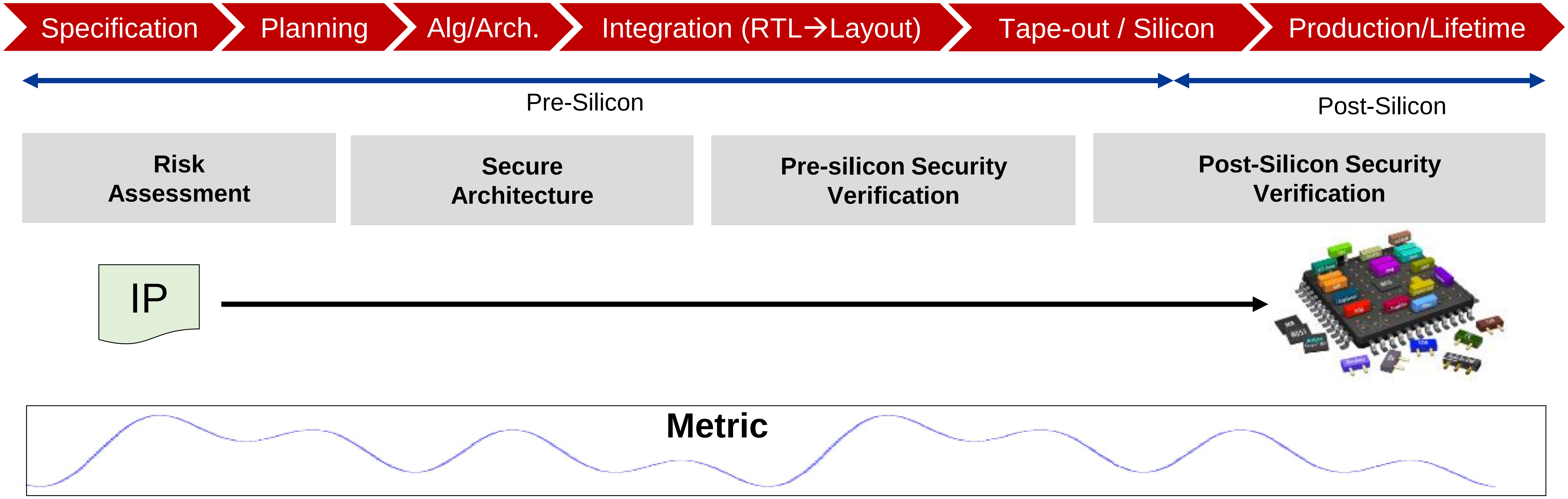


Hardware & Firmware Self Authentication



Quantifiable Assurance

Metrics throughout SDL



Specification → Planning → Alg/Arch. → Integration (RTL→Layout) → Tape-out / Silicon → Production/Lifetime

Pre-Silicon

Post-Silicon

Risk Assessment

Secure Architecture

Pre-silicon Security Verification

Post-Silicon Security Verification

Metric at IP-level tends to change while traversing through the design stages to the Platform in Silicon

Recommendation

Recommendation

- **Comprehensive Hardware Vulnerability Database**
- **Designed-in security Standards**
  - **Metrics, Standards**
- **Design with life cycle in mind**
  - **Device → Systems**
  - **Traceability & provenance**
- **Hardware Upgrade → Zero day**
- **Automation**
  - **Reduce complexity & cost**

Contact

Caspia is hiring!

careers@caspiatechnologies.com

www.caspiatechnologies.com

www.linkedin.com/company/caspia-technologies